IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

DOUGLAS E. TRENT, et al.

Serial No.:	09/666,804	Examiner:	William L. Bangachon
Filed:	21 September 2000	Art Unit:	2635
For:	PORTABLE SECURITY CONTAINER		

TRANMITTAL OF APPELLANT'S BRIEF FEE

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Accompanying this transmittal is a check drawn to the Commissioner of Patents and Trademarks in the amount of $250.00 for filing a Brief in support of a Notice of Appeal filed on 15th of November 2004. Should any additional fees be incurred, the Commissioner is authorized to charge Deposit Account No. 02-4943 in that amount. Please inform the Applicant of any transactions involving the Deposit Account.

Respectfully submitted,

Robert E. Bushnell
Reg. No.: 27,774

1522 "K" Street, N.W., Suite 300
Washington, D.C. 20005
Area Code: 202-408-9040

Folio: P56103C
Date: 15 February 2005
I.D.: REB/syk

PATENT
P56103C

IN THE UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

DOUGLAS E. TRENT, *et alii*

Serial No.:	09/666,804	Examiner:	WILLIAM L. BANGACHON
Filed:	21 September 2000	Art Unit:	2635
For:	PORTABLE SECURITY CONTAINER		

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O.Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to Appellant's Notice of Appeal filed on the 15th of November 2004, Appellant hereby appeals to the Board of Patent Appeals and Interferences from the final rejection of claims 1 through 49, as set forth in the final Office action mailed on the 13th of July 2004 (Paper No. 11).

Folio: P56332
Date: 2/15/05
I.D.: REB/kf

I. REAL PARTY IN INTEREST

Pursuant to 37 CFR §41.37(c)(1)(*i*) as amended), the real party in interest is:

MySpace, LLC
Post Office Box 1397,
Salem, VIRGINIA 24153-1397,

as evidenced by the Assignment executed by all three of the joint inventors on the 13th and 18th of December 2000 and recorded among the Assignment Record maintained by the United States Patent & Trademark Office on the 21st of December 2000 at Reel 011386, Frame 0312.

II. RELATED APPEALS AND INTERFERENCES

In conformance with 37 CFR §41.37(c)(1)(*ii*), there are no other appeals and no interferences known to Appellant, Appellant's legal representatives or the assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Pursuant to 37 CFR §41.37(c)(1)(*iii*), claims 1 through 49 are on appeal.

IV. COPY OF CLAIMS

In compliance with 37 CFR §41.37(c)(1)(*viii*), a copy of the claims involved in this appeal are contained in the Appendix.

V. STATUS OF AMENDMENTS

Pursuant to 37 CFR §41.37(c)(1)(*iv*), no Amendment was filed subsequent to the final Office action mailed on the 13th of July 2004 (Paper No. 11). On, or about, the 15th of November 2004 Appellant filed a written Response to the final Office action (Paper No. 11). No amendments to the claims were offered in this Response. To date, Appellant has received no correspondence from the Office in reply to this Response.

VI. SUMMARY OF CLAIMED SUBJECT MATTER

Circuit For Container Management System

Pursuant to 37 CFR §41.37(c)(1), Figures 1 and 2 illustrate details of one embodiment of a container management system that may be constructed in accordance with the principles of the present invention, with a host computer 100 driving a video monitor 90 to display varying visual images and symbols, and a keyboard 98 that enables a user to manually enter information and commands into computer 100. A data cable 102 such as a serial cable, a parallel multi-lead cable, a small computer system interface (*i.e.*, a SCSI) cable, a universal serial bus (*i.e.*, a USB) cable, or one or more optical fibers, is coupled at one end into a conforming socket operationally connected to the motherboard of computer 100, and terminated at the opposite end by a plug 104 that may be removably inserted into a socket 128 that is operationally coupled, by for example, a ribbon cable 130 that provides a data bus, to a microprocessor based controller 120. Information received by controller from host computer 100 may be written into and read from a non-volatile memory 121 that is addressed by controller 120.

Motion Sensor

A motion sensor 170 may be mounted either upon circuit board 122, or within container 110, to provide motion signals to controller 120 whenever sensor 170 detects movement of container 110. Senor 170 may be implemented with a spring loaded switch designed to provide motion signals that exhibit one logic state when container 110 is stationary upon a desktop, for example, with the juxtaposition of the container and the desktop holding the actuator of the switch depressed, and a second and different logic state when container 110 is lifted above the desktop and the actuator of the switch is released. Alternatively, motion sensor 170 may detect changes in inertia and provide a motion signal to controller 120 whenever container 110 is in motion.

Location Sensor

A location sensor such as, by way of example, a global position satellite receiver stage 172 and its antenna 174 mounted to extend externally to container 110, may be periodically polled by controller 120 to furnish a relatively accurate indication of the geographic location of container 110. Controller 120 may be programmed to refuse to deny access to container 110, by way of example, refusing to release an electro-mechanical latch whenever receiver stage 172 fails to indicate that container 110 is located at an assigned location.

Structure Of Portable Container

As illustrated in Fig. 2, the portable container 110 may be constructed with one or more sidewalls 112 forming an outer casement 109 closed at one end by a continuous bottom surface 116. An inner casement 118 for container 80 may be constructed with one or more sidewalls 84 jointed together and closed at one end by a continuous bottom surface 82. The upper rim 86 of

container 110 may be extended outward to engage the inner surfaces 88 and sidewalls 112, thereby providing a cavity 19 between the spaced apart sidewalls 84 and inner surfaces 88 that may be used to accommodate a circuit board 122, lead cable 130 and socket 128. An aperture 114 formed on one of the sidewalls 112 exposes socket 128 to an environment external to a container 110. A lid, or other panel 84 encloses both the inner and outer containers, once inner container 118 has been inserted between sidewalls 112 of outer container 70, and controls access to the interior of inner casement 80 and thus container 110. When panel 84 completely engages the sidewalls 112 of outer casement 109, access to the interior of container 110 may be utterly denied; when panel 84 is dislodged from this complete engagement however, full access may be permitted into the interior.

Regulation For Control Of Access

An electro-mechanical latch 163 operated by controller 120 may be mounted within container 110 to restrict removal of access panel 84, and thereby preserve the unrestricted access to the contents of container 110 while panel 84 remains undisturbed in its complete engagement of lower container 70. Controller 120 regulates application of an electrical current to relay R1 to control whether the contact wiper of the switch S1 component of relay R1 is opened or closed, and whether electrical current is applied to solenoid L1. In the absence of electrical current through solenoid L1, that is, when switch S1 is in its electrically open state, a spring 167 may be used to bias the armature 168 to extend axially outward along the central axis defined by the coil winding of solenoid L1, and engage the aperture 168 formed in a hasp 169 mounted on the underside of panel 84. When controller 120 directs relay R1 to close switch S1 and apply an electrical current

to the winding of solenoid L1, the armature of solenoid L1 is withdrawn from aperture 168, as is shown in Fig. 1, to release hasp 169 and allow removal of panel 84. Optionally, in mechanical lock 162 such as a cylinder lock rotatably operated with a bitted key, may be mounted on the outer casement 70 at a location enabling lock 162 to engage lid 84 and thereby provide an additional degree of security when lock 162 is turned into its locked position. It should be noted that although circuit board 122 is mounted upon one of the several sidewalls 84 of the inner casement 80, it is also feasible to mount circuit board 122 beneath floor 82, and between outer floor 116 and inner floor 82, or, alternatively, to distribute the components mounted upon circuit board 122 into various distinct and different locations within the container, and even upon a underside of access panel 84.

Electrical Power For Container

Nominally, circuit board 122 may be powered directly by a power cord 50 with a jack 52 received within a socket 54 mounted upon circuit board 122. A power supply 56 coupled to socket 54, may be used to rectify, filter, attenuate and distribute electrical power to rechargeable battery 58 mounted upon circuit board 122, as well as to electro-mechanical latch 163, controller 120 and transceiver 136, alarm 162, motion sensor 170 and location sensor 172, among other elements supported by circuit board 122.

Communication Network For Container And Host Terminal

Turning now to Figs. 3 through 8, communication between host computer 100 and controller 120, or alternatively, a local computer 100 or a computer 101 sited at a remote location to which container 110 has been transported, may be conducted in various modalities, depending

upon which aperture within container 110 is serving as a port (*e.g.*, an industry standard personal computer socket 128 (*e.g.*, a serial port socket, a parallel port socket, a SCSI I or SCSI II socket, or a universal serial bus socket), infrared transmitter and receiver unit 154, radio or microwave length antenna 134, or global positioning satellite antenna 174) to accommodate transmission of data signals between a host external to container 110, such as computer 100, 101, and the controller 120 encased within container 110. A multi-lead data cable 102 terminated by plug 104 may couple either a parallel port, a serial port, a small computer system interface port, or universal serial bus port of computer 100 to bus 130 and controller 120 via socket 128. Alternatively, a data cable 150 coupled to an infrared transmitter 152 may communicate via line-of-site to infrared transmitter 154 that may be mounted in aperture 114, or within a different aperture, to receive communications from infrared transmitter 152. Preferably, an infrared transmitter and infrared receiver unit 152 would be used to communicate with an infrared transmitter and infrared receiver unit 154 coupled to controller 120 via data bus 150. Alternatively, computer 100 may drive radio frequency or microwave transmitter and receiver unit 106 via data cable 105, to propagate radio frequency or microwave signals via antenna 108. Portable container 110 may be fitted with retractable antenna 134 to receive the radio frequency wave signals propagated from antenna 108, or alternatively, a microwave antenna to receive microwave signals. Antenna 134 may be coupled to controller 120 via transmitter and receiver unit 136. Consequently, and regardless of whether data cable 102 is simply a direct electrical or optical connection with an output port of computer 100, 101, or a category 5 local area network, the conduction of transmission of data signals via port 128 is dependent upon the disposition of container 110 relative to the source (*e.g.*, personal

computer 110, 101) of the data signals. By way of example, if container 110 is moved away from the neighborhood of data cable 102, the limited length of data cable 102 will ultimately cause jack 104 to unplug from socket 128, thereby interrupting the conduction of transmission of data signals via port 128. Assuming that infrared transmitter and receiver unit 154 is serving as the port however, movement of container 110 relative to host computer 100, 101 to a location that would remove the line-of-sight alignment between infrared units 152, 154 will cause an interruption in the conduction of transmission of data signals via port 154. Should antenna 134 serve as the port for communications between computer 100, 101 however, movement of container 110 relative to computer 100, 101 to a location where either intervening electrical conductors, attenuation of signal strength due to distance, or removal of antenna 134 from the field of antenna 108 will cause an interruption in the conduction of transmission of data signals via port 134.

Application Of Information And Signals To Control Time, Location And Personnel For Grant Of Access

The interruption of the conduction of transmission of data signals via the selected port, or ports, provided by container 110 may be used, together with one or more schemes for transmission of data signals (including transmission of a data key to authorize access to the interior of container 110), as well as the content of the data signals transmitted, to restrict and control access to the interior of container 110. If, for example, antenna 174 is serving as the port accommodating conduction of transmission of data signals, movement of container 110 to a geographic location outside of the authorized range of siting (*e.g.*, assuming that the global positioning system has a range of ± 30 feet, movement of container 110 to a location more than thirty feet from the location

authorized by computer 100 will be readily discernable by controller 120 from the position signal provided by GPS stage 172) is a factor that may be used by controller 120, in conjunction with host computer 100, in a scheme to control access to the interior of container 110. Accordingly, in response to a request for access entered via keyboard 96 and transmitted by one, or more, of the ports 128, 134, 154, and 174 provided by container 110, controller makes a determination of whether to grant the access requested by generating a control signal that allows lock 162 to release the access panel 84 on the basis of, *inter alia*, the disposition of the port relative to a source of the data signals, on the basis of the disposition of the container within a scheme for generation of the data signals, and in response to occurrence of a coincidence between a data key received by controller 120 among the data signals via the port and a data sequence obtained by controller 120 in dependence upon the information stored within memory 121.

Interruption Of Communications

Interruption of communications between computer 100 and controller 120 mounted on, or within, container 110, regardless of whether the interruption of communication occurs by removal of plug 104 from socket 124, severance of data cable 102, movement of container 110 to prevent transmission of signals between infrared units 152, 154, or interference with or suppression of signals between antennas 108, 134, may be used to trigger either alarm unit 160 driven directly by computer 100, or alarm 162 mounted on, or within container 110 and driven directly by controller 120, or alternatively, by both alarm units 160, 162, to broadcast a sensible alarm indicating the interruption of communication.

Input Of Information And Signals To Container

Although Fig. 1 shows container 110 fitted with separate data socket 128 and power socket 54, these sockets may be combined into a single socket 128 receiving both electrical power and either optical or electrical signals from plug 104. Additionally, container 110 may be fitted with a keypad or other manually operable switches 180 to enable container 110 to communicate with controller 120 independently of keyboard 98 and computer 100. This may be useful, for example, to power-up controller 120 or alternatively, to initiate a transmission from controller 120 to computer 100. Additionally, container 110 may be fitted with a visual or aural status indicator 182 such as a light-emitting diode that either flashes, is intermittently illuminated or is illuminated with different colors to indicate the status such as "no fault" or, no unauthorized movement or to indicate an unauthorized attempt to gain access to the contents of container 110. A touch memory port 184 may also be fitted into container 110 to enhance security, by way of example, to enable controller 120 to obtain a thumb print or a finger print from a prospective user and compare the print obtained via touch memory port 184 with a print of the prospective user that is stored in memory 124. Additionally, and as illustrated in Fig. 7, either or both host computer 100, or the computer 101 sited at the designation of container 110 may be operationally coupled to maintain communications with portable container 110 via line-of-sight infrared transmissions 55. A biometric scanner 188 may be connected to computer 100 as a peripheral unit to provide an enhanced degree of security, particularly when used together with a magnetic or optical strip card reader 186. Together, biometric scanner 188, card reader 186 and keyboard 98 allow the input of the three items of security information from each prospective user of container 110 essential to a rigid security scheme, namely who the prospective user is (*e.g.*, via biometric scanner 188), what

the prospective user has possession of (*e.g.*, namely an access card bearing a magnetic or optical strip confirming the authorization of the bearer to obtain access to the interior of container 110), and what the prospective user knows (*e.g.*, a data key known to the prospective user that may be entered via keyboard 98). Authentication of these items of information by computer 100, 101, enables the computer to communicate with controller 120 borne by container 110 and authorize controller 120 to allow the user to gain access to the interior of container 110, as, for example, by energizing solenoid L1 to release access panel 84.

VII. REFERENCES OF RECORD

U.S. Patents

- Porter, U.S. Patent No. 5.774.053
- Bates, U.S. Patent No. 6.057.779
- Gokcebay, U.S. Patent No. 5.254.329

VIII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Rejection of Claims 23-28 Under First Paragraph Of 35 U.S.C. §112

Claims 23 through 28 are rejected under the first paragraph of 35 U.S.C. §112, based upon the Examiner's question of whether the application, as originally filed, complied with the requirement of the first paragraph of 35 U.S.C. §112 for a written description of Appellant's *times scheme for generation of data signal.*

2. Rejection Of Claims 1-6, 10-18, 22 And 29-32 Under 35 U.S.C. §102(b)

Claims 1 through 6, 10 through 18, 22 and 29 through 32 are finally rejected under 35 U.S.C. §102(b) as anticipated by Porter, U.S. Patent No. 5.774.053.

3. **Rejection Of Claims 7-9, 19-21 And 23-28 Under 35 U.S.C. §103(a)**

Claims 7 through 9, 19 through 21 and 23 through 28 are finally rejected under 35 U.S.C. §103(a) as rendered obvious, and unpatentable, by Porter, U.S. Patent No. 5.774.053.

4. **Rejection Of Claims 33-48 Under 35 U.S.C. §103(a)**

Claims 33 through 48 are finally rejected under 35 U.S.C. §103(a) as rendered obvious, and unpatentable, by the Examiner's proposed combination of Porter, U.S. Patent No. 5.774.053, modified according to Bates, U.S. Patent No. 6.057.779.

5. **Rejection Of Claim 49 Under 35 U.S.C. §103(a)**

Claim 49 is finally rejected under 35 U.S.C. §103(a) as rendered obvious, and unpatentable, by the Examiner's proposed combination of Porter, U.S. Patent No. 5.774.053, modified according to Bates, U.S. Patent No. 6.057.779 and Gokcebay U.S. Patent No. 5.254.329.

IX. ARGUMENT

1. **Rejection of Claims 23-28 Under First Paragraph Of 35 U.S.C. §112**

Claims 23 through 28 are rejected under the first paragraph of 35 U.S.C. §112, based upon the Examiner's question of whether the application, as originally filed, complied with the requirement of the first paragraph of 35 U.S.C. §112 for a written description of Appellant's *times scheme for generation of data signal*? The application, as originally filed, describes the details

of a network that provides for a *timed scheme for generation of data signals*?[1]

Claims 23 through 28 were amended [2] to shift one phrase, and clarify the relation between the frequencies (wavelength) of the data signals and the carrier signals. This conforms to the Detailed Description beginning with page 11, which contemplates the transmission of data signals via fixed wire or via other modes, or the transmission of data signals superimposed upon carrier signals in the radio frequency, microwave or optical wavelength bands. As now written, claim 23 defines, *inter alia*, a *timed scheme for generation of data signals*. This conforms to the Summary of the Invention, beginning on page 4, and continuing on page 5, of granting access:

> "on the basis of the disposition of the container within a scheme for generation of the data signals",[3]

which is further described in the Detailed Description in terms of:

> "Access to the portable containers in the system may be ... ***time and date dependent*** in addition to user or control point verifications. Features such as dual control ... and time delay (a wait period after

---

1 Claim 23, as amended, line 13.

2 Claim 23 was amended in Appellant's Amendment filed on the 23rd of April 2004 to add the clause "in dependence upon disposition of said port relative to a source of said data signals and in dependence upon disposition of said container within a *timed scheme for generation of said data signals*" which currently appears in lines 11-13.

3 "In response to a request for access ... transmitted by one, or more, of the ports provided by the container, the controller makes a determination of whether to grant the access requested by generating a control signal that allows the lock to release the access panel on the basis of, *inter alia*, the disposition of the port relative to a source of the data signals, on the basis of the disposition of the container within ***a scheme for generation of the data signals***, and in response to occurrence of a coincidence between a data key received by the controller among the data signals via the port and a data sequence obtained by the controller in dependence upon the information stored within the memory." Summary *Of The Invention*, beginning with line 17, page 4 and continuing through line 3 on page 5.

> verification before ... allows access) are available"[4],

and,

> "The foregoing paragraphs describe details of a container management system that advantageously provides a portable lock with an authentication component that may be time, date, geographic and person dependent ...";[5]

as well as,

> "In essence, controller 200 regulates access to the contents of box 110 by controlling moving element 400, and allows access on the basis of date delivered via adaptor 300. Optionally, controller 200 may ... optionally make access decisions based upon the status of clock 205."[6]

In other words, the specification as originally filed contemplates the control of access to a container regulated according to *generation of data signals* such as signals bearing an authentication component, and optionally, controlling that generation of data signals on the basis of time or date.

The office of the specification is to provide an explanation of the details enabling another to practice the principles of Appellant's invention,[7] and is not an *ipsa verbis* repetition of the

---

4 "Access to the portable containers in the system may be geographic (as represented by global position satellite signals), ***time and date dependent*** in addition to user or control point verifications. Features such as dual control (requiring more than one user to be verified) ***and time delay*** (a wait period after verification before locking mechanism 163 in container 110 allows access) are available." Original specification, page 17, lines 14 through 18, emphasis added.

5 Original specification, page 18, lines 10 and 11.

6 Original specification, page 19, line 21, and page 20, lines 1 through 3.

7 "This detailed description, required by 37 CFR §1.71, *MPEP* §608.01, must be in such particularity as to enable any person skilled in the pertinent art or science to make and use

verbatim language of the claims.[8] Accordingly, in view of the foregoing demonstration, Appellant's originally filed specification presents a written description of regulating access according to a scheme for controlling the generation of data signals and for controlling that generation on the basis of time, **or** on the basis of date. There is no basis for sustaining this rejection of claims 23 through 28; such action is respectfully requested.

Rejection of Claims 1-6, 10-18, 22-25 and 29-32 Under 35 U.S.C. § 102(b)

Claims 1 through 6, 10 through 18, 22 through 25 and 29 through 32 were rejected in Paper No. 11 for a second and final time under 35 U.S.C. § 102(b) as anticipated by Porter U.S. Patent No. 5,774,053. This rejection should no be sustained.

First, the Examiner has incorrectly asserted that Porter '053 "teaches a container manager" that contains that exact language of Appellant's claim 1. Despite the thorough reading, the exact language of Appellant's claim 1 is absent from the printed text of Porter '053. The completeness mandated by 37 C.F.R. §1.104(a)(b) and (c) is not provided by the Examiner's explanation of Porter '053. Although Appellant made a timely written request to the Examiner for clarification, none has been given by the Examiner.

- By way of example, the Examiner was requested to explain precisely which portion

---

the invention without undue experimentation." *MPEP* §608.01(g), Rev. 1 (August 2001)

[8] "The function of the [written] description requirement is to ensure that the inventor had possession of, as of the filing date of the application relied on, the specific subject matter later claimed by him or her; ***how the specification accomplishes this is not material.***" *MPEP* §2106.01, Rev. 2 (May 2004).

of Porter '053 teaches Appellant's "control stage being mounted entirely within and being completely encased by said container during said complete engagement" of "a closed interior while said lid is in complete engagement with said housing."[9]

- The Examiner was also requested to identify precisely where Porter '053 teaches that any port (48) of Porter '053 accommodates "conduction of transmission of data signals ***between*** said closed interior and an environment external to said housing" as defined by Appellant's claim 1.[10]

In a disjointed and incomplete response, in Paper No. 11 the Examiner has written that "lock operator 24 mounted inside of the front door 18" is "entirely within and being encased by the container (lid) as claimed" [11] and that,

> "lock operator [24] in this case is the control stage because the lock operator, coupled with the keypad and controller {Porter, col. 2, lines 30-36},[12] controls the locking and unlocking of the front door (lid) {Porter, col. 2, lines 25-29}."[13]

---

9 Claim 1, lines 9-11.

10 Claim 1, lines 6-8.

11 Contrary to the inference advanced by the Examiner, the location of Appellant's "movable latch" is not a feature of claim 1.

12 Porter '053, column 2, lines 29-35 reads: "The preferred communication apparatus includes a controller coupled with the keypad and lock operator and a transmitting device responsive to the controller. The controller includes conventional memory for storing a plurality of vendor codes each associated with a separate vendor and a plurality of vendor messages each associated with one of the vendor codes."

13 Paper No. 11, page 5. Porter '053, column 2, lines 25-29 reads: "the enclosure includes a door, a lock for locking the door, and a lock operator for unlocking the lock. In preferred forms, the lock operator includes a keypad for permitting the entry of a plurality of keycodes."

This superficial effort to show anticipation ignores the close conformity between the teachings of Porter '053 about the relation between "controller 46" and "lock operator 24", namely that "controller 46 directs the lock operator 24 to unlock the door 18,"[14] and Appellant's definition of,

> "a movable latch disposed to engage said lid and hinder removal of said lid from said complete engagement, and to respond to said control signal by releasing said lid from said complete engagement."[15]

Regardless of whether the Board accepts or rejects the Examiner's efforts to bundle "controller 46" and "lock operator 24" together, it is important to keep sight of the Examiner's impetus for this bundling, which was the Examiner's statement that:

> "The Examiner gladly provides an explanation in response to applicant's request for clarification as to which portion of Porter teaches a) 'said ***control state (stage)*** being mounted entirely within and being completely encased by said container during said complete engagement ... of a closed interior while said lid is in complete engagement with said housing' and b) 'conduction of transmission of data signals between said closed interior and an environment external to said housing'"[16]

because the Examiner has, in this piecemeal consideration of claim 1, lost sight of (*i*) the fact that neither "the keypad" nor the "controller" may be read as "being mounted entirely within and being completely encased by said container during said complete engagement"[17] and the fact that (*ii*) the clause "conduction of transmission of data signals between said closed interior and an environment

---

[14] Porter '053, column 6, lines 11 and 12.

[15] Claim 1, lines 18-20.

[16] Paper No. 11, page 5.

[17] Paper No. 11, page 5.

external to said housing" appears in the definition of Appellant's "port"[18] rather in Appellant's definitions of "a control stage" or "a movable latch."[19]

The Examiner's citation of column 6, lines 16 thorough 28 of Porter '053 [20] as teaching "a port (48) borne by said housing and exposed through said housing to accommodate conduction of transmission of data signals between said closed interior and an environment external to said housing" is equally inadequate, because this passage of Porter '053 and the accompanying Figures 1, 2, 3 and 4 simply discusses "transmitting device 48" externally mounted on the exterior of Porter '053's "storage device 10", and fails to disclose any port[21] accommodating "conduction of data signals" in combination of "a control stage ... mounted entirely with and being completely encased by said container during said complete engagement"[22] or "a control stage ... generating a

---

18 Claim 1, lines 6-8.

19 The Examiner has also lost sight of Appellant's request for clarification specified an identification of where Porter '053 taught "that any ***port*** (48) of Porter '053 accommodates 'conduction of transmission of data signals ***between*** said closed interior and an environment external to said housing' as defined by Appellant's claim 1."

20 Paper No. 11, page 10.

21 Ignored in the Examiner's assertion is (*i*) the fact that Figure 5 of Porter '053 shows transmitting device 48 as a constituent of communication apparatus 16 which Figures 1, 2, 3 and 4 all consistently show on the exterior of "storage device 10" and (*ii*) the fact that Appellant's claim 1 distinguishes between the *control signal* to which Appellant's "movable latch" responds and the *data signals* for which Appellant's port is said "to accommodate conduction of transmission ... between said closed interior and an environment external to said housing." Claim 1, lines 6-8.

22 Claim 1, lines 9-11.

control signal in dependence upon disposition of said port relative to a source of said data signals" [23] or "a control stage ... generating a control signal ... in dependence upon disposition of said container within a scheme for generation of said data signals"[24] or "a control stage ... generating a control signal ... in response to occurrence of a coincidence between a data key received among said data signals via said port ... ."[25] In fact, transmitting device 48 is, as is "controller/computer 46", clearly shown in Figure 1 through 4 of Porter '053 as being mounted external to the "interior" of the container. The external mounting of communication assembly 48 by Porter '053 leaves its communication apparatus 48 subject to external tampering without Appellant's securing of the communication apparatus within the closed interior.[26] Moreover, Porter '053 nowhere uses the term "port" to define communication apparatus 48, and in effect, the Examiner has mislabeled the structure of Porter '053 in an effort to demonstrate anticipation. Under 35 U.S.C. §102, it is error to assume that two structures are the same or equivalent simply because those structures may perform the same function. The United States Court of Appeals for the Federal Circuit has held that it is error to assume that two structures are the same or equivalent simply because they may perform the same function. *Roton Barrier, Inc. v. Stanley Works,* 79 F.3d 1112, 1126-27 (Fed. Cir.

---

23 The Examiner has ignored the teaching of Porter '053 that ostensibly, storage device 10 is stationery.

24 Claim 1, lines 13 and 14.

25 Claim 1, lines 14 and 15.

26 Claim 1, lines 9-12 reads "a control stage ... being mounted entirely within and being completely encased by said container during said complete engagement, and being operationally coupled to provide communication with said interior via said port ... ."

1996); *Pennwalt Corp. v. Durand-Wayland, Inc.*, 833 F.2d 931, 934 (Fed. Cir. 1987) (en banc) ("Pennwalt erroneously argues that, if an accused structure performs the function required by the claim, it is per se structurally equivalent"), *cert. denied,* 485 U.S. 961 (1988). Anticipation is found only if the identical invention is "shown in as complete detail as is contained in the ... claim."[27] Neither the externally mounted "transmitting device 48" of Porter '053, which does not disclose any port accommodating any communication between the closed interior and an environment external to the housing, nor any other disclosed component of Porter '053 teaches Appellant's "container manager" with, among other features, "a port ... exposed through said housing to accommodate conduction of transmission of data signals between said closed interior and an environment external to said housing" or Appellant's "control stage being mounted entirely with and being completely encased by said container during said complete engagement."[28] Absent the teaching by Porter '053 of each and every element set forth in claim 1, there is no anticipation.

Claim 13

Independent claim 13 defines, *inter alia*, "a control stage" that is "mounted entirely within said container."[29] The Examiner neglects to address this feature of claim 13, among other features of claim 13, in the Examiner's comments on page 8 of Paper No. 11. The Examiner has failed to satisfy the degree of completeness required by 37 C.F.R. § 1.104. Appellant has made written

---

27 *Manual of Patent Examining Procedure*, 8th Ed., Rev. 2 (May 2004), citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1566 (Fed. Cir. 1990).

28 Claim 1, lines 6-11.

29 Claim 13, lines 8 and 9.

requests under 37 C.F.R. § 1.104(c)(2) for the Examiner to explain where Porter '053:

- teaches a "control stage being mounted entirely within said container", in the combination defined by claim 13
- teaches a control stage "complete encased by said container during said complete engagement", in the combination defined by claim 13.

The absent of clarifying demonstration of these features in Porter '053 in satisfaction of 37 C.F.R. §1.104 by identifying the specific elements relied upon to support this rejection, buttresses the foregoing demonstration of a lack of a teaching or suggestion by the prior art of the subject matter of the pending claims in their entiries.

Claim 29

Claim 29 defines, among other features, an alarm "driven in response to an ***unauthorized interruption of said communication via said port.***" Paper No. 7 does not address this feature, and although Appellant requested clarification, the art fails to:

- explain which specific part of Porter '053 teaches Appellant's alarm "driven in response to an unauthorized interruption" of said communication, in the combination defined by claim 29.
- identify the specific part relied upon in Porter '053 to teach the generation of any alarm in response to "interruption of" communication via a port "exposed through said housing to receive data signals", in the combination defined by claim 29.

Absent such features of the pending claims, this rejection of claim 29 should not be sustained..

Rejection of Claims 7-9, 19-21 and 26-28 Under 35 U.S.C. §103 (a)

Claims 7 through 9, 19 through 21, and 26 through 28 are finally rejected under 35 U.S.C. §103(a) as rendered obvious, and unpatentable by Porter '053. This rejection fails to make a *prima facie* showing of obviousness.

First, as earlier noted, Porter '053 is devoid of any teaching of either Appellant's "port" as defined by parent pending claims 1, 13 and 23, or by Appellant's "control stage" that is, "mounted entirely within" and "complete encased by the container during the complete engagement" as defined by parent claims 1 and 13. Under the all-elements-rule, withdrawal of this rejection is required.

Second, in support of the rejection, the Examiner has simply paraphrased the language of the rejected claims, without bothering to discern that the reference numbers of Porter '053 are not associated with the text of Appellant's claims anywhere within the specification of Porter '053. This impermissible attribution of the language of Appellant's claims to the text of Porter '053 is improper, and fails to consider the requirement under 35 U.S.C. §103(a) that obviousness is determined on the subject matter of Appellant's invention *in its entirely*, as defined by the claims, rather by a paraphrased of those claims. Moreover, this explanation of the Examiner's application of particular components of Porter '053 to individual components of the rejected claims, fails to address the cooperation of those features which is spread across two or more paragraphs of each claim. In essence, the application of Porter '053 to the claims is little more than an aggregation of parts that are unrelated in the manner defined by Appellant's claims. This application of Porter '053, by ignoring Appellant's inter-cooperation between elements of the claims, fails to provide

the degree of completeness required by 37 C.F.R. §1.104(b) and (c). Porter' 053 does not even use the noun "port" (although other references of record to) and demonstrates no relation between a "port" and either a "closed interior" or a "controller. Simply identifying discrete components of Porter '053, and failing to combine those components in a manner defined by the claims, does not demonstrate obviousness. The rejection is therefore unsustainable.

Third, as previously explained, the mounting of the control stage "entirely within said container" provides a degree of security and resistance to tampering unavailable with Porter '053. In view of this distinction and the advantage flowing therefrom, these claims are patentably distinguishable and allowable over Porter '053.

Rejection of Claims 33-48 under 35 U.S.C. §103(a)

Claims 33 through 48 were again rejected under 35 U.S.C. §103 with the verbatim reasoning set forth in the first Office action, as rendered obvious by a proposed combination of Porter '053 modified according to Bates U.S. Patent No. 6,057,779. Appellant respectfully traverses this rejection for the following reasons.

As applied to support the rejection of claims 33 and 34, the Examiner's proposed combination incorporates a geographically selective locking scheme of Bates '779 that is dependent upon a global positioning satellite communications link. The Examiner's discussion of "different frequencies" is irrelevant to the scope of these claims, and ignores the fact that the Examiner's proposed combination lacks Appellant's "alarm driven in response to an unauthorized ***interruption of said communication by said port*** to broadcast an indication of said unauthorized

interruption" as defined by parent claim 29. This feature advantageously preserves the integrity of Appellant's container manager, a feature absent from the Examiner's proposed combination. In view of this distinction and the advantage flowing therefrom, claims 33 and 34 are patentably distinguishable over the proposed combination. Moreover, absent this feature in the proposed combination, there is no *prima facie* showing of obviousness.

Claims 35 through 41 and 47

In the Examiner's proposed combination, communication device 32 of Bates '779 is connected via a RS-232 cable to lock controller 24, as is explained in column 4, beginning with line 39. This is essential to the implementation of the Examiner's proposed combination with the TPS received taught by the secondary reference. In contradistinction however, Appellant's "control stage" is "mounted entirely within and' is "completely encased by said container during said complete engagement", a feature neither recognized nor appreciated by the Examiner's proposed combination. In fact, neither the primary nor secondary reference appreciates the enhancement of security attributable to this feature. Absent this, there is neither *prima facie* showing of obviousness nor other basis for maintaining the rejection.

Moreover, the fact that the primary and secondary references singularly ignore this feature is itself convincing indicia of non-obviousness. Such evidence may not be ignored under 35 U.S.C. § 103. Accordingly, there is no basis for sustaining this rejection and allowance of claims 35 through 49.

Rejection of Claim 49 under 35 U.S.C. § 103(a)

Claim 49 is finally rejected under 35 U.S.C. § 103(a) as rendered obvious, and unpatentable, over a proposed combination of Porter '053 modified according to Bates '779 and Gokcebay U.S. Patent No. 5,254,329. This rejection is improper and fails to make a *prima facie* showing of obviousness under 35 U.S.C. § 103(a).

The Examiner's Proposed Combination Enables One Seeking Access To Wholly Control Input Of The Data Upon Which An Allowance Of Access Is Based.

Claim 49 defines a structure that uses

> "said control stage being mounted entirely within and being completely encased by said container during said complete engagement"

in combination with,

> "a source of an *input signal* representing a *first class of information*, mounted upon and borne by said housing;
>
> a port borne by said housing and exposed through said housing to accommodate conduction of transmission of *data signals* through said housing;
>
> a control stage comprised of a memory storing a *second class of information* specific to said container, said control stage being mounted entirely within and being completely encased by said container during said complete engagement, and being operationally coupled to provide communication with said interior via said port, and generating a control signal in dependence upon disposition of said port relative to an origin of said *data signals*, in dependence upon said information represented by said *input signal*, and in response to occurrence of a coincidence between a *data key* received among said data signals via said port and a *data sequence* obtained by said control stage in dependence upon said *information stored* within said memory ... ."

Consequently, individual seeking access is unable to supply all of the data and information upon

which the decision to grant, or withhold, access is based. In the Examiner's proposed combination incorporating Gokcebay '329 however, all of the biometric data must be entered concurrently entered by the user seeking access via wall-mounted control panel 28 which must be located at access control point 12, in single, or sequential arrangement with different security levels, to[30] control entry (*see,* column 8, beginning with line 58, together with column 5, line 59). This modification of the primary reference consequently depends upon a site-comparison between concurrent entry of both data borne by the card-type or bitted key 16, and "includes information specific to the intended key holder" which is also entered via a "reader panel 28 shown in FIG. 3." As illustrated in its FIG. 3, the Examiner's proposed combination including Gokcebay '329 necessarily requires that to obtain a concurrent, on-site comparison between the data borne by the card-type or bitted key 16, and the "information specific to the intended key holder" that is entered concurrently with the data borne by key 16, both sets of data must be entered via "reader panel 28 shown in FIG. 3", and "reader panel 28 shown in FIG. 3." In essence, in the Examiner's proposed combination, the user seeking access controls the entry of all information, and therefore, controls the content of that information to the controller regulating access; so long as there is a coincidence between the biometric data fed to "key reader 26" and the biometric data fed to "scanner 42" [31], and the key is being used within its allotted window of time, access to the keyholder is granted. In contradistinction, in claim 49,

---

[30] Gokcebay '329, col. 7, lines 23.

[31] See Gokcebay '329, Figures 3, 4 and 5, together with column 7, lines 9 through 14 and lines 23 through 28.

> a control stage comprised of a memory storing a *second class of information* specific to said container ... ."

This advantageously enable the shipper of the container to control both (*i*) the input and (*ii*) the content of Applicant's *second class of information*, as well as (*iii*) the timing of the entry of that *second class of information*, upon which the determination to grant access may be based. As explained in claim 49, that *second class of information* may in a particular embodiment, comprise biometric information. This is a degree of control provided to the shipper, or to the owner, or to the consignee, of the container that is not available with the Examiner's proposed combination, which advantageously enhances the degree of security provided to the contents of the container. In view of these distinctions, and the enhanced degree of security provided by these distinctions, there is no *prima facie* showing of obviousness.

The Examiner's Proposed Combination Is Keyholder Specific, And Thus Fails To Make A *Prima Facie* Showing Of Obviousness.

In the Examiner's proposed combination, the Examiner asserts that,

> "Gokcebay teach [*sic*, teaches] a second class of information comprising **biometric data**."[32]

That data is carried both by the keyholder's key 16 and by the keyholder's body (in the form of a physical characteristic of the keyholder). A decision to grant, or to deny, access is then made based upon a comparison of these two forms of the same biometric data for the keyholder.[33] In

---

[32] Paper No. 11, paragraph 18, page 18.

[33] See Gokcebay '329, at column 9, beginning with line 67 and continuing through column 10, line 10.

essence, in the Examiner's proposed combination, all classes of data upon which the decision to grant access is specific to the keyholder, regardless of whether the keyholder is legitimate or an imposter. In contradistinction, claim 49 defines, *inter alia*,

> "a control stage comprised of a memory storing a *second class of information* specific to said container ... ."

Recognizing that all classes of information used in the Examiner's proposed combination are necessarily specific to the keyholder, that proposed combination fails to make a *prima facie* showing of obviousness, and should not be sustained.

The Examiner's Proposed Combination Does Not Enhance The Security Provided To The Controller Governing Access.

As previously noted, the primary reference exposes its controller 46 and its associated "communication apparatus 16" to the vagaries of the exterior of its "storage device 10." Incorporation of Gokcebay '329 to the Examiner's proposed combination ignores the distinctions explained in the foregoing paragraphs, that are included within dependent claim 49. By way of example, Gokcebay '329 depends on externally, wall-mounted control panel 28 at access control point 12, in single, or sequential arrangement with different security levels, to[34] control entry (*see,* column 8, beginning with line 58, together with column 5, line 59). This modification of the primary reference depends upon a site-comparison between concurrent entry of both data borne by the card-type or bitted key 16, and "includes information specific to the intended key holder" which is also entered via a "reader panel 28 shown in FIG. 3." As illustrated in its FIG. 3, the

---

[34] Gokcebay '329, col. 7, lines 23.

Examiner's proposed combination including Gokcebay '329 necessarily requires that to obtain a concurrent, on-site comparison between the data borne by the card-type or bitted key 16, and the "information specific to the intended key holder" that is entered concurrently with the data borne by key 16, both sets of data must be entered via "reader panel 28 shown in FIG. 3", and "reader panel 28 shown in FIG. 3" must be exposed to the exterior of any space to which access is controlled. It is this exposure on the exterior of the controlled space, together with the fact that Central Processing Unit 15 which provides "door opening" in the Examiner's proposed combination is utterly unprotected by access control point 12, limits the degree of security because the Examiner's proposed combination makes no effort to (*i*) limit the amount of data an unauthorized user is able to enter at access control point 12 via key reader 26 and scanner 42, or (*ii*) to protect Central Processing Unit 15 from tampering. In contradistinction, claim 49 defines a structure that uses

> "said control stage being mounted entirely within and being completely encased by said container during said complete engagement."

This feature is not found in the Examiner's proposed combination. In fact, none of the references forming the Examiner's proposed combination either recognizes the advantages of this feature or seek to implement this feature, is convincing indicia of obviousness *vel non*. Accordingly, this rejection can not be sustained.

SUMMARY

Recalling the rejection of claims 23 through 28, the function of the requirement for a *written*

description under the first paragraph of 35 U.S.C. §112 is to ensure that the inventor had possession of, as of the filing date of the application relied on, the specific subject matter later claimed by him or her; ***how the specification accomplishes this is not material.***[35] Where the specification originally filed expressly states that a grant of access may be made:

> "on the basis of the disposition of the container within a scheme for generation of the data signals",[36]

and the originally filed specification further describes that access in terms of:

> "Access to the portable containers in the system may be ... ***time and date dependent*** in addition to user or control point verifications. Features such as dual control ... and time delay (a wait period after verification before ... allows access) are available"[37],

then the specification provides a written description for an implementation of these principles with Appellant's step of granting access:

---

35 *MPEP* §2106.01, Rev. 2 (May 2004).

36 "In response to a request for access ... transmitted by one, or more, of the ports provided by the container, the controller makes a determination of whether to grant the access requested by generating a control signal that allows the lock to release the access panel on the basis of, *inter alia*, the disposition of the port relative to a source of the data signals, on the basis of the disposition of the container within ***a scheme for generation of the data signals***, and in response to occurrence of a coincidence between a data key received by the controller among the data signals via the port and a data sequence obtained by the controller in dependence upon the information stored within the memory." Summary *Of The Invention*, beginning with line 17, page 4 and continuing through line 3 on page 5.

37 "Access to the portable containers in the system may be geographic (as represented by global position satellite signals), ***time and date dependent*** in addition to user or control point verifications. Features such as dual control (requiring more than one user to be verified) ***and time delay*** (a wait period after verification before locking mechanism 163 in container 110 allows access) are available." Original specification, page 17, lines 14 through 18, emphasis added.

> "in dependence upon disposition of said container within ***a timed scheme for generation of the data signals.***"[38]

The Board is respectfully urged to acknowledge the presence of this written description, and to refuse to sustain this rejection.

---

38 "In response to a request for access ... transmitted by one, or more, of the ports provided by the container, the controller makes a determination of whether to grant the access requested by generating a control signal that allows the lock to release the access panel on the basis of, *inter alia*, the disposition of the port relative to a source of the data signals, on the basis of the disposition of the container within ***a scheme for generation of the data signals***, and in response to occurrence of a coincidence between a data key received by the controller among the data signals via the port and a data sequence obtained by the controller in dependence upon the information stored within the memory." Summary *Of The Invention*, beginning with line 17, page 4 and continuing through line 3 on page 5.

Turning to the questions of anticipation under 35 U.S.C. §102(b) based upon Porter '053, and of obviousness under 35 U.S.C. §103(a) based upon either Porter '053, or combinations of Porter '053 and Bates '779 or of Porter '053, Bates '779 and Gockebay '329, it suffices to note that the pending claims fails to either teach or to recognize the advantage of an enhancement of security flowing from Appellant's step of simply also encasing, and thereby protecting the security of the controller which makes the decision to grant, or to deny, access to Appellant's container through the expedient of,

> "a control stage comprised of a memory storing information specific to said container, said control stage being mounted entirely within and being completely encased by said container during said complete engagement,"

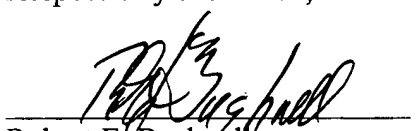
a feature neither suggested by the various items of prior art advanced in support of the final rejections. [39] This defect in both Porter '053 as well as Bates '779 deprives the controller of the proposed combination Appellant's protection against tampering provided by the interior of the container being secured, a marked departure from the teachings of Appellant's claims 1, 13, 23, 29 and 35. Moreover, the fact that the Examiner's interpretations of the art enables an imposter seeking access to wholly control the input of all of the data, either directly as taught by Gokcebay '329 or by enabling tampering of the controlling microprocessor which makes the determination to grant, or

---

[39] This omission in the Examiner's several proposed combinations is buttressed by the teaching of the secondary reference, Bates '779, in column 4, lines 39 through 41, which requires that "system 10 further includes a remote intelligent communications device 32 9FIG. 3) supported by the vehicle 12 and in communication with the lock 22." This communications device 32, together with its transmitter 39, receiver 38, cpt 33, EPROM 34 and RAM 34 are mounted on the outside of mobile container 12, and are thus receives none of the protection against tampering provided by the interior of container 12, a marked departure from the teachings of Appellant's claims 1, 13, 23, 29 and 35.

deny, access, which is, in the prior art, deprived of the protection of the secured container, is a further and additionally patentably distinguishing feature not found in the Examiner's proposed combinations. In view of these omissions, deficiencies and differences in the prior art and the finally rejected claims, the Board is urged to refuse to sustain the several final rejections of claims 1 through 49.

Respectfully submitted,



Robert E. Bushnell
Attorney for the Appellant
Reg. No.: 27,774

1522 "K" Street, N.W.,
Suite 300
Washington, D.C. 20005
202-408-9040

Folio: P56103C
Date: 2/15/05
I.D.: REB/kf

APPENDIX

In compliance with 37 CFR §41.37(c)(1)(*viii*), the claims, as finally rejected, are:

1. (Original) A container manager, comprising:

a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement;

a port borne by said housing and exposed through said housing to accommodate conduction of transmission of data signals between said closed interior and an environment external to said housing;

a control stage comprised of a memory storing information specific to said container, said control stage being mounted entirely within and being completely encased by said container during said complete engagement, and being operationally coupled to provide communication with said interior via said port, and generating a control signal in dependence upon disposition of said port relative to a source of said data signals, in dependence upon disposition of said container within a scheme for generation of said data signals, and in response to occurrence of a coincidence between a data key received among said data signals via said port and a data sequence obtained by said control stage in dependence upon said information stored within said memory; and

a moveable latch disposed to engage said lid and hinder removal of said lid from said complete engagement, and to respond to said control signal by releasing said lid from said complete engagement.

2. (Original) The container manager of claim 1, further comprised of a socket mounted within said housing providing said port.

3. (Original) The container manager of claim 1, further comprised of an infrared receiver mounted within said housing providing said port.

4. (Original) The container manager of claim 1, further comprised of an antenna mounted within said housing providing said port.

5. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key; and

a data cable coupling said host computer to said port.

6. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key; and

a local area network coupling said host computer to said port.

7. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key;

said port comprising a first antenna mounted on one of said sidewalls;

a data transceiver connecting said first antenna and said controller; and

a second antenna driven by said host computer, operationally connecting said host computer to said first antenna.

8. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key;

an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data key; and

an infrared receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter.

9. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key;

a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and

a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter, and to transmit operational communications from said controller to said host computer via said first infrared transmitter and receiver.

10. (Original) The container manager of claim 1, further comprised of:

said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port; and

an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal.

11. (Original) The container manager of claim 1, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, periodically making a determination of whether said an unauthorized interruption of said communication has occurred; and

an alarm driven by said host computer to broadcast an indication of said unauthorized interruption in dependence upon said determination.

12. (Original) The container manager of claim 1, further comprised of:

said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port;

a first alarm driven by said host computer to broadcast an indication of said unauthorized interruption in response to said alarm signal;

a microprocessor based host computer operationally coupled to said controller via said port, periodically making a determination of whether said an unauthorized interruption of said communication has occurred; and

a second alarm driven by said host computer to broadcast an indication of said unauthorized interruption in dependence upon said determination.

13. (Original) A container manager, comprising:

a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement;

a port mounted within said housing and exposed through said housing to receive data signals;

a control stage comprised of a memory storing information specific to said container, said control stage being mounted entirely within said container, being completely encased by said container during said complete engagement, and being operationally coupled to provide communication by data signals with said interior via said port, and generating an alarm

signal in response to an unauthorized interruption of said communication via said port; and

an alarm driven by said controller to broadcast an indication of said unauthorized interruption in response to said alarm signal.

14. (Original) The container manager of claim 13, further comprised of a socket mounted within said housing providing said port.

15. (Original) The container manager of claim 13, further comprised of an infrared receiver mounted within said housing providing said port.

16. (Original) The container manager of claim 13, further comprised of an antenna mounted within said housing providing said port.

17. (Original) The container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals; and

a data cable coupling said host computer to said port while conveying said data signals to said controller via said port.

18. (Original) The container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via

said port, generating said data signals; and

a local area network coupling said host computer to said port while conveying said data signals to said controller via said port.

19. (Original) The container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals;

said port comprising a first antenna mounted on one of said sidewalls;

a data transceiver connecting said first antenna and said controller; and

a second antenna driven by said host computer, operationally connecting said host computer to said first antenna while conveying said data signals to said controller via said first antenna.

20. (Original) The container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals;

an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data signals; and

an infrared receiver mounted in one of said sidewalls, disposed to receive and convey to said controller said data signals from said infrared transmitter.

21. (Original) The container manager of claim 13, further comprised of:

a microprocessor based host computer operationally coupled to said controller via said port, generating said data key;

a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and

a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter, and to transmit operational communications from said controller to said host computer via said first infrared transmitter and receiver.

22. (Original) The container manager of claim 14, further comprised of:

said controller generating a control signal in response to occurrence of a coincidence between a data key received via said port and a data sequence obtained by said control stage in dependence upon information stored within said memory; and

an electromechanical latch responding to said control signal by hindering removal of said lid from said complete engagement.

23. (Previously Presented) A container manager, comprising:

a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said

lid is dislodged from said complete engagement;

a port exposed through one of said sidewalls to receive data signals;

a control stage comprised of a memory, said control stage being mounted on said container and being operationally coupled to provide communication with said interior via said port, and generating a control signal in response to occurrence of a coincidence between a data key received among said data signals via said port and a data sequence obtained by said control stage in dependence upon information stored within said memory, in dependence upon disposition of said port relative to a source of said data signals and in dependence upon disposition of said container within a timed scheme for generation of said data signals;

a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals; and

an electromechanical latch disposed to engage said lid and hinder removal of said lid from said complete engagement, and to respond to said control signal by releasing said lid from said complete engagement.

24. (Original) The container manager of claim 23, further comprised of a data cable coupling said host computer to said port.

25. (Original) The container manager of claim 24, further comprised of a local area

network coupling said host computer to said port.

26. (Original) The container manager of claim 25, further comprised of:

said port comprising a first antenna mounted on one of said sidewalls;

a data transceiver connecting said first antenna and said controller; and

a second antenna driven by said host computer, operationally connecting said host computer to said first antenna.

27. (Original) The container manager of claim 26, further comprised of:

an infrared transmitter driven by said host computer to broadcast an infrared signal corresponding to said data key; and

an infrared receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter.

28. (Original) The container manager of claim 27, further comprised of:

a first infrared transmitter and receiver driven by said host computer to broadcast an infrared signal corresponding to said data key; and

a second infrared transmitter and receiver mounted in one of said sidewalls, disposed to receive said data key from said infrared transmitter, and to transmit operational communications from said controller to said host computer via said first infrared transmitter and receiver.

29. (Original) A container manager, comprising:

a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, said housing providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement;

a port exposed through said housing to receive data signals;

a control stage comprised of a memory, said control stage being mounted on said container and being operationally coupled to provide communication by data signals with said interior via said port;

a microprocessor based host computer sited externally to said container, said host computer comprising a keyboard initiating formation of said data signals and a monitor driven by said host computer to visually display video images, said host computer being operationally coupled to said port and participating in said communication by generating said data signals; and

an alarm driven in response to an unauthorized interruption of said communication via said port to broadcast an indication of said unauthorized interruption in response to said alarm signal.

30. (Original) The container manager of claim 29, further comprised of:

said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port; and

said alarm being driven by said control stage to broadcast an indication of said unauthorized interruption in response to said alarm signal.

31. (Original) The container manager of claim 29, further comprised of:

said host computer periodically making a determination while operationally coupled to said controller via said port, of whether said an unauthorized interruption of said communication has occurred; and

an alarm driven by said host computer to broadcast an indication of said unauthorized interruption in dependence upon said determination.

32. (Original) The container manager of claim 29, further comprised of:

said controller generating an alarm signal in response to an unauthorized interruption of said communication via said port;

a first alarm driven by said host computer to broadcast an indication of said unauthorized interruption in response to said alarm signal;

said host computer periodically making a determination while operationally coupled to said controller via said port, of whether said an unauthorized interruption of said communication has occurred; and

a second alarm driven by said host computer to broadcast an indication of said unauthorized interruption in dependence upon said determination.

33. (Previously Presented) The container manager of claim 29, further comprised of:

said data signals exhibiting a first wavelength, and said data signals exhibiting a second and different wavelength carrier signal; and

said port being plug coupleable to said control stage, and comprising a transmitter stage converting said data signals into output signals exhibiting said second wavelength, and a receiver stage converting said data signals into input signals exhibiting said first wavelength.

34. (Previously Presented) The container manager of claim 29, with said port comprised of:

a first unit that is plug coupleable to said control stage when said data signals by said control stage exhibit a first wavelength and said data signals by said exhibit a second and different wavelength carrier signal, said first unit comprising a receiver stage converting said data signals received by said port into input signals exhibiting said first wavelength, and a transmitter stage converting said data signals provided by said control stage into output signals exhibiting said second wavelength; and

a second unit that is plug coupleable to said control stage and interchangeable with said first unit to provide a data connection between said control stage and said host computer when said data signals received by said port exhibit the same wavelength as said data signals provided by said control stage.

35. (Original) A container manager, comprising:

a housing comprised of a plurality of sidewalls bearing a removable lid, forming a container having a closed interior while said lid is in complete engagement with said housing, and providing an open interior able to removably receive items within said open interior while said lid is dislodged from said complete engagement;

a source of an input signal representing a first class of information, mounted upon and borne by said housing;

a port borne by said housing and exposed through said housing to accommodate conduction of transmission of data signals through said housing;

a control stage comprised of a memory storing a second class of information specific to said container, said control stage being mounted entirely within and being completely encased by said container during said complete engagement, and being operationally coupled to provide communication with said interior via said port, and generating a control signal in dependence upon disposition of said port relative to an origin of said data signals, in dependence upon said information represented by said input signal, and in response to occurrence of a coincidence between a data key received among said data signals via said port and a data sequence obtained by said control stage in dependence upon said information stored within said memory; and

a latch mounted on said housing and disposed to engage said lid and hinder removal of said lid from said complete engagement, and to respond to said control signal by releasing said lid from said complete engagement.

36. (Original) The container manager of claim 35, further comprised of said source detecting movement of said lid, and said first class of information indicating said movement.

37. (Original) The container manager of claim 35, further comprised of said source detecting a position of said lid, and said first class of information indicating said position.

38. (Original) The container manager of claim 35, further comprised of said control stage generating said control signal in response to instructions received by said control stage from said host computer independently of said disposition of said port, independently of said information represented by said input signal, and independently of said occurrence of coincidence.

39. (Original) The container manager of claim 35, further comprised of said control stage generating said control signal in dependence of said disposition of said port, in dependence of said information represented by said input signal, in dependence of said occurrence of coincidence, and in response to instructions received by said control stage from a host computer coupled to said port.

40. (Original) The container manager of claim 35, further comprised of said container being transportable between an origin and a destination, and said data key being encoded and being available only at destination.

41. (Original) The container manager of claim 35, further comprised of said container being transportable between an origin and a destination, and said data key being encoded and being transmitted to said port from said origin.

42. (Original) The container manager of claim 35, further comprised of said container being transportable between an origin and a destination, and said data key being encoded and being available only at destination.

43. (Original) The container manager of claim 35, further comprised of a microprocessor based host computer operationally coupled to said controller via said port, generating said data signals.

44. (Original) The container manager of claim 43, further comprised of said host computer comprising a cellular telephone bearing a graphical user interface.

45. (Original) The container manager of claim 35, further comprised of some or all of said data signals being transmitted across or received one of an Internet and a wide area network.

46. (Original) The container manager of claim 35, further comprised of said data signals comprising one of an e-mail packet and an attachment to an e-mail message.

47. (Original) The container manager of claim 35, further comprised of said information represented by said source comprising a global location of the container, and said control stage generating said control signal in dependence of said disposition of said port, in dependence of said information represented by said input signal, and in dependence of said occurrence of coincidence.

48. (Original) The container manager of claim 35, further comprised of said container being transportable between an origin and a destination, and a user at one of said origin and said destination requests via a network a request for some part of said data key.

49. (Original) The container manager of claim 35, further comprised of said container being transportable between an origin and a destination, and said second class of information is installed at said origin comprises biometric data matching a person of a human user of said container and said coincidence must be made with biometric data matching said person at said destination.